

Shigenaga discloses:

- Card terminal generating a random number and encrypts twice;
- Card terminal sending encrypted data to card IC;
- Card IC decrypting the encrypted data and determines the random number;
- Card IC sending determined random number back to card terminal; and,
- Card terminal comparing both the time of processing, and the original and received random numbers to determine authenticity.

Thus, when one compares Shigenaga with the "Authenticate Card Routine 300" disclosed in Lee, which is discussed in more detail below, it is apparent that the cited documents are totally different. For example:

- Shigenaga teaches encrypting the random number prior to sending to card, whereas in contrast to Lee which teaches sending the random number unencrypted;
- Shigenaga teaches decrypting in the card IC, whereas in contrast Lee fails to teach decrypting in the card IC to authenticate the card;
- Shigenaga teaches sending the random number back to the terminal in unencrypted form, whereas in contrast Lee teaches sending the random number to the host in encrypted form; and,
- Shigenaga teaches that the terminal compares the received data to the stored random number, whereas in contrast Lee teaches that the data needs to be unencrypted prior to comparison.

Therefore, with such a large number of contrasting features of the respective systems, the applicant submits that a skilled person in the art would simply not be motivated to combine Shigenaga with Lee.

Furthermore, Shigenaga suggests that it is essential that the authentication is performed by comparing the actual processing time with the estimation processing time. Lee fails to suggest any such feature. Therefore, it is submitted that a person skilled in the art would simply not be motivated to combine Shigenaga which relies on comparing processing times with Lee which simply compares random numbers.

Additionally, a skilled person in the art would not be motivated to combine Shigenaga with Lee since both are directed to encrypting and decrypting random numbers at totally opposite ends of the system (ie. at the host or at the card).

There is no suggestion or motivation in either Lee or Shigenaga that two opposing authentication techniques could be combined since there is a large number of contrasting features. Additionally, there is no suggestion or motivation in the knowledge generally available to one of ordinary skill in the art that a public key used for encrypting could also be used for decrypting data for authenticating an untrusted authentication chip. Furthermore, there is no suggestion or motivation in the knowledge generally available to one of ordinary skill in the art that a private key used for decrypting could also be used for encrypting data for authenticating an untrusted authentication chip.

Therefore, there is no motivation to combine Shigenaga with Lee for authenticating an untrusted authentication chip.

In any event, if Shigenaga was combined with Lee, obviousness can only be established by combining or modifying teachings of the prior art to produce the claimed invention where there is some teaching, suggestion or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art.

On pages 3 to 4 of the Office Action, the Examiner has stated:

*"Shigenaga does not disclose applying, in the trusted authentication chip, a key one way function to the second decrypted outcome using the second key to produce an encrypted outcome...Lee discloses the IC card performs both encrypt and decrypt function using an internal key stored in the card and the terminal card performs both encrypt and decrypt function using an identifying key stored in memory (column 6, lines 37-67)"*

However, on closer inspection of the section of Lee which the Examiner has highlighted, in fact Lee describes two **separate routines that are performed separately**.

In particular, lines 37 to 52 describes the "Authenticate Card Routine 300" which is used for "allow[ing] system 100 to determine whether a card inserted into one of the card units is authentic" (Column 6, lines 37 to 40). The "Authenticate Card Routine 300" comprises the steps of:

- a processor 122 generating a random number (column 6, lines 40 and 41);
- processor 122 transmits generated random number to the card (column 6, line 41);
- card receives random number; (column 6, lines 41 to 42);
- card encrypts random number using algorithm and an "internal key" (column 6, lines 42 to 43);
- card returns encrypted random number to processor 122 (column 6, line 44);
- processor 122 decrypts the encrypted number based upon same algorithm and an identifying key (column 6, lines 46 to 48); and
- processor 122 compares the original random number to the decrypted random number to determine authenticity of the card (column 6, lines 48 to 50).

In contrast to the "Authenticate Card Routine 300", as described by Lee, and outlines above, claim 1 of the present application describes:

- applying in the trusted authentication chip a keyed one way function to a random number by using a first key, thereby producing a first encrypted outcome.
- applying in the untrusted authentication chip a keyed one way function to the random number using a second key, thereby producing a second encrypted outcome.
- comparing the first encrypted outcome and the second encrypted outcome, without knowledge of the first or second key.

Thus, as shown in the comparison above, Lee does not describe having a first and a second encrypted outcome produced by the trusted and untrusted authentication chips respectfully, where the first and second encrypted outcomes are compared in order to determine whether the untrusted authentication chip is valid. In Lee, the processor in the Authenticate Card Routine 300 compares the original random number to the decrypted random number in order to determine the authenticity of the card.

Additionally, Lee does not describe the application of a first and a second key in the trusted and untrusted chips respectfully to produce the first and second encrypted outcomes. Lee only encrypts the random number once, in the processor, the random number is then returned to the card, and is decrypted. Lee does not describe separately encrypting the random numbers thereby producing two separate encrypted outcomes.

Furthermore, the Applicant highlights to the examiner that claim 1 describes comparing the first and second encrypted outcomes without knowledge of the first and second keys. In the Authenticate Card Routine 300 of Lee, the processor first decrypts the encrypted random number received based upon an algorithm and an identifying key stored in the memory 126, before comparing the original random number to the decrypted random number. Thus, the processor has knowledge of at least one key, which is in contrast to the validation protocol of claim 1.

Thus, claim 1 of the present invention provides numerous distinctions between a combination of Shigenaga and Lee.

In a totally separate routine as shown in Figure 3, Lee describes at column 6, lines 53 to 65 the "Authenticate Host Routine 310" which is used *"to allow a card to determine whether the processing system in which the card is inserted is authentic"*. Thus, Lee describes that this routine is used by the card to determine the authenticity of the host.

Therefore "Authenticate Card Routine 300" is in total contrast to "Authenticate Host Routine 310" because "Authenticate Card Routine 300" is used for authenticating the card whereas "Authenticate Host Routine 310" is used for authenticating the host. Nowhere in Lee is it suggested that these two routines could be combined to only authenticate the card.

In any event, the routine for authenticating the host, as described by Lee, is in contrast to the present claim 1 for similar reasons as described above with respect to the card authentication routing 300.

The host authentication routine 310 does not describe having a first and a second encrypted outcome produced by the trusted and untrusted authentication chips respectfully, where the first and second encrypted outcomes are compared in order to determine whether the untrusted authentication chip is valid. In Lee, the card in the Authenticate Card Routine 310 compares the original random number to the decrypted random number in order to determine the authenticity of the processor. Furthermore, the routine 310 in Lee does not describe the application of a first and a second key in the trusted and untrusted chips respectfully to produce the first and second encrypted outcomes.

Thus, lines 37 to 67 of column 6 which the Examiner has highlighted are irrelevant to the claims. Accordingly, the combined teachings of lines 37 to 67 in column 6 of Lee and the disclosure of Shigenaga fail to teach or suggest the features of claim 1 as outlined above.

The Applicant respectfully submits that in authentication systems, these are not trivial distinctions, and claim 1 is patentable over a combination of Shigenaga and Lee.

The MPEP states at 2143 "*Basic Requirements of a Prima Facie Case of Obviousness*" that:

*"... three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.*

*The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)."*

Thus as Shigenaga and Lee fail to teach or suggest the limitations of:

- applying in the trusted authentication chip a keyed one way function to a random number by using a first key, thereby producing a first encrypted outcome.
- applying in the untrusted authentication chip a keyed one way function to the random number using a second key, thereby producing a second encrypted outcome.
- comparing the first encrypted outcome and the second encrypted outcome, without knowledge of the first or second key.

The applicant submits that independent claims 1 and 6 are patentable over Shigenaga in view of Lee as required by MPEP at 2143.

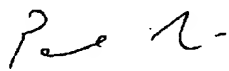
The applicant respectfully requests that Examiner withdraw the rejection to all the claims.

In view of the foregoing, it is respectfully requested that the Examiner reconsider and withdraw the rejections under 35 U.S.C. §103(a). The present application is believed to be in condition for allowance. Accordingly, the Applicant respectfully requests a Notice of Allowance of all the claims presently under examination.

Very respectfully,

Applicants:

  
\_\_\_\_\_  
SIMON ROBERT ALMSLEY

  
\_\_\_\_\_  
PAUL LAPSTUN

C/o: Silverbrook Research Pty Ltd  
393 Darling Street  
Balmain NSW 2041, Australia  
Email: [kia.silverbrook@silverbrookresearch.com](mailto:kia.silverbrook@silverbrookresearch.com)  
Telephone: +612 9818 6633  
Facsimile: +61 2 9555 7762